Foundations of Cryptography
Fall Semester 2011—2012
Exercise 3

Peleg Michaeli

1st February 2012

Section a

We prove the following lemmas:

Lemma 1. *Let $x, c \in \{0,1\}^m$, $x \neq 0^m$, and let A be chosen uniformly from $\mathbb{F}_2^{m\times n}$. Then: $\mathbb{P}\left(Ax = c\right) = \frac{1}{2^m}$.*

Proof. Since $x \neq 0^m$ there exists a regular matrix[1] R for which $Rx = e_1$. Since R is regular, AR is also distributed uniformly over $\mathbb{F}_2^{m\times n}$ (since R is simply a permutation of A). Hence,

$$\mathbb{P}\left(Ax = c\right) = \mathbb{P}\left(ARx = c\right) = \mathbb{P}\left(Ae_1 = c\right)$$

The condition $Ae_1 = c$ simply means that the first (leftmost) column of A is c. This leaves us $mn - m$ degrees of freedom (to choose elements of A), hence

$$\mathbb{P}\left(Ax = c\right) = \frac{2^{mn-m}}{2^{mn}} = 2^{-m}$$

as we wished to show. □

Lemma 2. *Let $x \in \{0,1\}^m$, and let A be chosen uniformly from $\mathbb{F}_2^{m\times n}$ and d chosen uniformly from $\{0,1\}^m$. Then: $\mathbb{P}\left(Ax = d\right) = \frac{1}{2^m}$.*

Proof. Using the complete probability formula, we obtain:

$$\mathbb{P}\left(Ax = d\right) = \sum_{t\in\{0,1\}^m} \frac{1}{2^m}\mathbb{P}\left(Ax = t\right)$$

[1] A regular matrix is a matrix whose determinant is not 0.

In the case where $x \neq 0^m$, the previous lemma shows that $\mathbb{P}(Ax = t) = 2^{-m}$, and we get

$$\mathbb{P}(Ax = d) = 2^m \cdot \frac{1}{2^m} \cdot \frac{1}{2^m} = \frac{1}{2^m}$$

as wanted. In the case where $x = 0$, $\mathbb{P}(Ax = t) = \mathbb{P}(0 = t)$, which is 0 unless $t = 0$, in which case it is 1, which gives

$$\mathbb{P}(Ax = d) = \frac{1}{2^m} \cdot 1 = \frac{1}{2^m}$$

as wanted. This completes the proof. □

Corollary 3. *Let $x, y \in \{0,1\}^m$, and let A be chosen uniformly from $\mathbb{F}_2^{m \times n}$ and b chosen uniformly from $\{0,1\}^m$. Then: $\mathbb{P}(Ax + b = y) = \frac{1}{2^m}$.*

Proof. Clearly $\mathbb{P}(Ax + b = y) = \mathbb{P}(Ax = y - b)$. Let $d = y - b$; then, d is also distributed uniformly over $\{0,1\}^m$, hence we can use the previous lemma to obtain our conclusion. □

We now prove the claim stated in the question.

$$\begin{aligned}
\mathbb{P}(h_{A,b}(x) = y \wedge h_{A,b}(x') = y') &= \mathbb{P}(h_{A,b}(x) = y \wedge h_{A,b}(x') - h_{A,b}(x) = y' - y) \\
&= \mathbb{P}(h_{A,b}(x) = y) \cdot \mathbb{P}(h_{A,b}(x') - h_{A,b}(x) = y' - y \mid h_{A,b}(x) = y) \\
&= \mathbb{P}(Ax + b = y) \cdot \mathbb{P}((Ax' + b) - (Ax + b) = y' - y \mid Ax + b = y) \\
&= 2^{-m} \cdot \mathbb{P}(Ax' + b = y') = 2^{-m} \cdot 2^{-m} = 2^{-2m}
\end{aligned}$$

as we wished to show.

Section b

g is clearly length-preserving. We will show, then, that g is a one-way function. For that, assume g is not such. If so, there is a polynomial $q(n)$ and a PPT algorithm A which, given y in the range of g, outputs some x, for which $\mathbb{P}\left(x \notin f^{-1}(y)\right) > 1/q(n)$ infinitely often. We will use that algorithm to contradict f's one-wayness.

We define an algorithm B as follows: B gets as input 1^n and $y \in \{0,1\}^{\ell(n)}$. At first step, B chooses a function h from $\mathcal{H}_n$ (efficiency of $\mathcal{H}$ allows that). We plug $(h(y), h)$ into A and get A's output (which we will now call r) – this is possible, since y is a proper input for the function h, and $(h(y), h)$ is a proper input for the algorithm A. The output r is of the form $r = (x, h')$ where $x \in \{0,1\}^{2n}$ and $h' \in \mathcal{H}_n$. At this stage, B checks x and returns its first n coordinates.

We now show that B "inverts" f. For that, we first prove the following proposition:

Proposition 4. *Given* $y \in \{0,1\}^{\ell(n)}$,

$$\mathbb{P}\left(B(1^n, y) \in f^{-1}(y)\right) \geq \mathbb{P}\left(A(h(y), h) \in g^{-1}(h(y), h) \wedge \forall y' (h(y) = h(y') \to y' = y)\right)$$

Proof. Suppose $A(h(y), h) \in g^{-1}(h(y), h) \wedge \forall y' (h(y) = h(y') \to y' = y)$. In particular, $g(a(h(y), h))$ equals $(h(y), h)$ and so $A(h(y), h)$ is of the form (x, h). We write $g(x, h) = (h(y), h)$ and conclude $h(y) = h(f(x_{1,\ldots,n}))$ (by g's definition). From the implication condition we obtain $y = f(x_{1,\ldots,n})$, where $x_{1,\ldots,n}$ is indeed the output of B, hence the inequality holds. $\square$

Though, the implication condition is rather cheap. To formalise, we show that the probability of this implication not to hold is negligible. Indeed, given y, and using union bound, we obtain

$$\mathbb{P}\left(\exists y' \left(y' \neq y \wedge h(y') = h(y)\right)\right) \leq \sum_{z \in f[\{0,1\}^n]} \mathbb{P}\left(y' \neq y \wedge h(y') = h(y)\right)$$

As $\mathcal{H}_n$ is a family of pairwise independent functions, $\mathbb{P}\left(y' \neq y \wedge h(y') = h(y)\right) = (2^{-2n})^2$, regardless of the choice of y'. Hence the sum on the right hand side is no higher than $2^n \cdot 2^{-4n}$, which is negligible. We plug that result into the previous proposition to obtain

$$\mathbb{P}\left(B(1^n, y) \in f^{-1}(y)\right) \geq 1/q(n) - \text{neg}\,(n)$$

which is absolutely not negligible, contradicting f's one-wayness.